Release Notes for the Industrial Ethernet 5000 Hardened Aggregator, Cisco IOS Release 15.2(2)EB2

First Published: April 14, 2016

Cisco IOS Release 15.2(2)EB2 runs on all Cisco Industrial Ethernet IE 5000 switches.

Cisco IOS Software Release 15.2(2)EB2 is part of the new software releases on Cisco IE 5000 Series Switches. This release delivers new software innovations in Industrial deployments that span across many technologies.

These release notes include important information about Cisco IOS Release15.2(2)EB2, and any limitations, restrictions, and caveats that apply to it.

You can download the switch software from this site (registered Cisco.com users with a login password):

http://software.cisco.com/download/navigator.html

Contents

- System Requirements, page 2
- Upgrading the Switch License, page 4
- Installation Notes, page 4
- Software Features, page 4
- Important Notes, page 6
- Caveats, page 8
- Documentation Updates, page 9
- Related Documentation, page 9
- Obtaining Documentation, Obtaining Support, and Security Guidelines, page 9

Cisco Systems, Inc.
www.cisco.com

System Requirements

- Hardware Supported, page 2
- Express Setup Requirements, page 3

Hardware Supported

Switch Models Supported

Model	Total Ports	SFP/SFP+ Uplinks[1]	SFP Fiber Ports	Copper 10/100/1000 PoE/PoE+ Ports	Software Image
IE-5000-12S12P-10G	28	4 (1G/10G)	12 (FE/GE)	12 (10/100/1000BaseT)	LAN Base[2]
IE-5000-16S12P	28	4 (1G)	12 (FE/GE)	12 (10/100/1000BaseT)	LAN Base[2]

1. Uplink ports can run at 1G or 10G mode depending on the SFP/SFP+ inserted.
2. Can be upgraded to IP Services at a fee. IP Services License Product Numbers are the following:

- L-IE5000-RTU= (Electronic SW License for IE5000 Switches)

SFP Modules Supported

The SFP modules are switch Ethernet SFP modules that provide connections to other devices. Depending on the switch model, these field-replaceable transceiver modules provide uplink or downlink interfaces. The modules have LC connectors for fiber-optic connections.

You can use any combination of the supported SFP modules.

Table 1 SFP Modules

Description	Description	Temperature Range*
SFP Modules:		
GLC-FE-100FX-RGD=	100Base-FX Multi Mode Rugged SFP	IND
GLC-FE-100LX-RGD=	100Mbps Single Mode Rugged SFP	IND
GLC-SX-MM-RGD=	1000Mbps Multi-Mode Rugged SFP (supported on gigabit SFP ports only)	IND
GLC-LX-SM-RGD=	1000Mbps Single Mode Rugged SFP (supported on gigabit SFP ports only)	IND
GLC-ZX-SM-RGD=	1000BASE-ZX Single Mode Rugged SFP (supported on gigabit SFP ports only)	IND
SFP-GE-L=	1000BASE-LX/LH SFP (DOM)	EXT
SFP-GE-S=	1000BASE-SX SFP (DOM)	EXT
SFP-GE-Z=	1000BASE-ZX Gigabit Ethernet SFP (DOM)	EXT
GLC-EX-SMD=	GE SFP, LC Connector, EX transceiver	EXT
GLC-BX-D=	1000BASE-BX SFP, 1490NM	COM
GLC-BX-U=	1000BASE-BX SFP, 1310NM	COM
GLC-FE-100LX=	100BASE-LX SFP for FE port	COM
GLC-FE-100BX-D=	100BASE-BX10-D SFP	COM
GLC-FE-100BX-U=	100BASE-BX10-U SFP	COM

GLC-FE-100FX=	100BASE-FX SFP for FE port	COM
GLC-FE-100EX=	100BASE-EX SFP (40km)	COM
GLC-FE-100ZX=	100BASE-ZX SFP (80km)	COM
CWDM-SFP-1xxx= (i.e., 1470, 1490, 1510, 1530, 1550, 1570, 1590, 1610)	CWDM SFP w/ DOM (8 channels)	COM
GLC-FE-100BX-URGD	100BaseBX10-U Rugged SFP module	COM
GLC-T[1]	1000BASE Copper SFP	COM
10G SFP+ Modules:	**Only supported on IE-5000-12S12P-10G**	
SFP-10G-SR-X	10GBASE-SR SFP+ transceiver module for MMF, 850-nm wavelength	EXT
SFP-10G-LR-X	10GBASE-LR/10GBASE-LW/OTU2e SFP+ transceiver module for SMF, 1310-nm wavelength	EXT
SFP-10G-SR	10GBASE-SR SFP+ transceiver module for MMF, 850-nm wavelength	COM
SFP-10G-LRM	10GBASE-LRM SFP+ transceiver module for MMF and SMF, 1310-nm wavelength	COM
SFP-10G-LR	10GBASE-LR SFP+ transceiver module for SMF, 1310-nm wavelength	COM
SFP-10G-LR-X	10GBASE-LR/10GBASE-LW/OTU2e SFP+ transceiver module for SMF, 1310-nm wavelength	COM
SFP-10G-ER	10GBASE-ER SFP+ transceiver module for SMF, 1550-nm wavelength	COM
SFP-10G-ZR	10GBASE-ZR SFP+ transceiver module for SMF, 1550-nm wavelength	COM
SFP-H10GB-CU1M	10GBASE-CU passive Twinax SFP+ cable assembly, 1 meter	COM
SFP-H10GB-CU3M	10GBASE-CU passive Twinax SFP+ cable assembly, 3 meters	COM
SFP-H10GB-CU5M	10GBASE-CU passive Twinax SFP+ cable assembly, 5 meters	COM
SFP-H10GB-ACU7M	10GBASE-CU active Twinax SFP+ cable assembly, 7 meters	COM
SFP-H10GB-ACU10M	10GBASE-CU active Twinax SFP+ cable assembly, 10 meters	COM

1. GLC-T is supported from a software standpoint. However, there are several caveats associated with GLC-T support (temperature derating, radiated immunity, PTP performance), which aren't unique to IE 5000. On IE-5000-12S12P-10G, uplink ports can run at 1G or 10G mode depending on SFP/SFP+ inserted.

Express Setup Requirements

Hardware

- 1 gigahertz (GHz) or faster 32-bit (x86) or 64-bit (x64) processor
- 1 gigabyte (GB) RAM (32-bit) or 2 GB RAM (64-bit)
- 16 GB available hard disk space (32-bit) or 20 GB (64-bit)

Software

- PC with Windows 7, or Mac OS 10.6.x
- Web browser (Internet Explorer 9.0, 10.0, and 11.0; or Firefox minimum version 25, recommended version 32) with JavaScript enabled
- Straight-through or crossover Category 5 or 6 cable

Express Setup verifies the browser version when starting a session, and it does not require a plug-in.

Upgrading the Switch License

The IE5000 is shipped with a Permanent “lanbase” license. This can be upgraded to an “ipservices” Evaluation or Permanent Right-To-Use (RTU) license using CLI commands.

Installation Notes

You can assign IP information to your switch by using these methods:

- Express Setup program, as described in the switch getting started guide.
- CLI-based setup program, as described in the switch hardware installation guide.
- DHCP-based autoconfiguration, as described in the switch software configuration guide.
- Manual assignment of an IP address, as described in the switch software configuration guide.

Software Features

For more information about the following new features for this release, please see the associated Configuration Guide here:
http://www.cisco.com/c/en/us/td/docs/switches/lan/cisco_ie5000/software/release/15-2_2_eb/configuration/guide/scg-ie5000.html

Right-to-Use License

“Right to Use” (RTU) is a trust based licensing scheme designed to make life easier for customers. It is designed to give customers the flexibility to upgrade, downgrade, or move the license for RMA purpose by using simple EXEC CLI commands. As this is a “trust” based scheme, customer can pay for a certain number of licenses in advance, and then activate these flexibly across a full range of switches deployed provided the number of licenses does not exceed that number at any given time.

There are 2 main types of licenses used for the IE5000 - “Evaluation” and “Permanent RTU (PRTU)”. An “Evaluation” license allows the customer to evaluate an image for 60 days at no cost. A “Permanent RTU” license is a paid license with no expiration. A user is prompted to change to a permanent license before the evaluation license expires, with periodic reminders. This license is “in-built” in the image just like the current “Evaluation License” in the CISL model, so customers do not need to connect to Cisco servers to get a license. A PRTU license is not tied to a particular hardware. It can be deactivated from the old/swapped out hardware and activated on the replacement switch using the CLI.

Secure Boot

- With the Secure Boot mechanism, software must be digitally signed and verified for authenticity and integrity prior to load and execution. This protects customers from running tampered software and safeguards revenue through software counterfeit protection.
- The switch can be booted only with a timed key using valid IOS image.
- Every IOS release will have the timing keys embedded inside the IOS image.

Dying Gasp

- If there is a loss of power to the switch, it sends out “Dying Gasp” messages to the OAM center to notify about the situation.
- These messages inform the downstream nodes about the loss of the switch, which helps routing recovery.

Smart Install

Smart Install is a plug-and-play configuration and software upgrade feature that provides zero-touch deployment for new switches. You can ship a switch to a location, place it in the network, and power it on with no configuration required on the device. For more information, see *Smart Install Configuration Guide* here:
http://www.cisco.com/c/en/us/td/docs/switches/lan/smart_install/configuration/guide/smart_install.html

Note IE 5000 can be a Smart Installation Director.

Limitations and Restrictions

You should review this section before you begin working with the switch. These are known limitations that will not be fixed, and there is not always a workaround. Some features might not work as documented, and some features could be affected by recent changes to the switch hardware or software.

Cisco IOS Limitations

- IP
- RADIUS
- SPAN and RSPAN
- Spanning Tree Protocol
- VLAN

IP

- When the rate of received DHCP requests exceeds 2,000 packets per minute for a long time, the response time might be slow when you are using the console.

  The workaround is to use rate limiting on DHCP traffic to prevent a denial of service attack from occurring. (CSCeb59166)

RADIUS

- RADIUS change of authorization (COA) reauthorization is not supported on the critical auth VLAN.

  There is no workaround. (CSCta05071)

SPAN and RSPAN

- When the RSPAN feature is configured on a switch, Cisco Discovery Protocol (CDP) packets received from the RSPAN source ports are tagged with the RSPAN VLAN ID and forwarded to trunk ports carrying the RSPAN VLAN. When this happens a switch that is more than one hop away incorrectly lists the switch that is connected to the RSPAN source port as a CDP neighbor.

  This is a hardware limitation. The workaround is to disable CDP on all interfaces carrying the RSPAN VLAN on the device connected to the switch. (CSCeb32326)

- CDP, VLAN Trunking Protocol (VTP), and Port Aggregation Protocol (PAgP) packets received from a SPAN source are not sent to the destination interfaces of a local SPAN session. The workaround is to use the **monitor session** *session_number* **destination** {**interface** *interface-id* **encapsulation replicate**} global configuration command for local SPAN. (CSCed24036)

Spanning Tree Protocol

- CSCtl60247

  When a switch running Multiple Spanning Tree (MST) is connected to a switch running Rapid Spanning Tree Protocol (RSTP), the MST switch acts as the root bridge and runs per-VLAN spanning tree (PVST) simulation mode on boundary ports connected to the RST switch. If the allowed VLAN on all trunk ports connecting these switches is changed to a VLAN other than VLAN 1 and the root port of the RSTP switch is shut down and then enabled, the boundary ports connected to the root port move immediately to the forward state without going through the PVST+ slow transition.

  There is no workaround.

VLAN

- If the number of VLANs times the number of trunk ports exceeds the recommended limit of 13,000, the switch can fail.

  The workaround is to reduce the number of VLANs or trunks. (CSCeb31087)

- When line rate traffic is passing through a dynamic port, and you enter the **switchport access vlan dynamic** interface configuration command for a range of ports, the VLANs might not be assigned correctly. One or more VLANs with a null ID appears in the MAC address table instead.

  The workaround is to enter the **switchport access vlan dynamic** interface configuration command separately on each port. (CSCsi26392)

- When many VLANs are configured on the switch, high CPU utilization occurs when many links are flapping at the same time.

  The workaround is to remove unnecessary VLANs to reduce CPU utilization when many links are flapping. (CSCtl04815)

Important Notes

- Express Setup Notes, page 7

Express Setup Notes

- This browser setting is recommended for speeding up the time required to display Express Setup from Microsoft Internet Explorer:
  1. Choose **Tools > Internet Options**.
  2. Click **Settings** in the Temporary Internet files area.
  3. From the Settings window, choose **Automatically**.
  4. Click **OK**.
  5. Click **OK** to exit the Internet Options window.
- The HTTP server interface must be enabled to display Express Setup. By default, the HTTP server is enabled on the switch. Use the **show running-config** privileged EXEC command to see if the HTTP server is enabled or disabled.

Beginning in privileged EXEC mode, follow these steps to configure the HTTP server interface:

	Command	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**ip http authentication {aaa | enable | local}**	Configures the HTTP server interface for the type of authentication that you want to use. • **aaa**—Enables the authentication, authorization, and accounting feature. You must enter the **aaa new-model** interface configuration command for the **aaa** keyword to appear. • **enable**—Enables the password, which is the default method of HTTP server user authentication. • **local**—Specifies the local user database, as defined on the Cisco router or access server.
Step 3	**end**	Returns to privileged EXEC mode.
Step 4	**show running-config**	Verifies your entries.

- Express Setup uses the HTTP protocol (the default is port 80) and the default method of authentication (the enable password) to communicate with the switch through any of its Ethernet ports and to allow switch management from a standard web browser.

  If you change the HTTP port, you must include the new port number when you enter the IP address in the browser **Location** or **Address** field (for example, http://10.1.126.45:184 where 184 is the new HTTP port number). Write down the port number through which you are connected. Use care when changing the switch IP information.

  If you are *not* using the default method of authentication (the enable password), you need to configure the HTTP server interface with the method of authentication used on the switch.

Beginning in privileged EXEC mode, follow these steps to configure the HTTP server interface:

	Command	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**ip http authentication {enable | local | tacacs}**	Configures the HTTP server interface for the type of authentication that you want to use. • **enable**—Enables the password, which is the default method of HTTP server user authentication. • **local**—Specifies the local user database, as defined on the Cisco router or access server. • **tacacs**—Specifies the TACACS server.
Step 3	**end**	Returns to privileged EXEC mode.
Step 4	**show running-config**	Verifies your entries.

Note If the Express Setup failed in the Web Browser, use the reset button to reset the switch to factor default

Caveats

The following sections provide information about caveats. You can click the issue number to view more information in the Cisco Bug Search tool (login required):

- Open Caveats, page 8

Open Caveats

Issue	Description	Workaround
CSCuu47423	When enabling STP on ENI port gets wrong error message.	None
CSCuu34062	Power supply temperature is not displayed accurately.	None
CSCuu91553	PortThresholds setsingle returns GS 0x9 rather than changing threshold.	None
CSCuv00886	During switch startup, the FPGA's PCIe interface initialization fails resulting in a bus error followed by an automatic reload of IOS.	None
CSCuu77754	Extra entries for uplink port in hulc Entity-MIB.	None

Resolved Caveats

Issue	Description
CSCuy13431	ICMP error packets may corrupt the following IPv4 or ARP frame. This occurs on IE 4000 and IE 5000 running Cisco IOS 15.2(2)EA, 15.2(2)EB or 15.2(4)EA. IE 4000 and IE 5000 switches were running Cisco IOS 15.2(2)EA, 15.2(2)EB or 15.2(4)EA.

Documentation Updates

- Related Documentation, page 9

Related Documentation

Installation, Configuration, Maintenance, and Operation Guides

http://www.cisco.com/en/US/products/ps11245/tsd_products_support_series_home.html

Online Help (available on the switch)

- Express Setup online help
- Device Manager online help

SFP Information

- Compatibility Information: www.cisco.com/en/US/products/hw/modules/ps5455/products_device_support_tables_list.html
- Installation Notes: www.cisco.com/en/US/products/hw/modules/ps5455/prod_installation_guides_list.html

MIBs

- MIBs can be located with this MIB tool by using the IOS version number: tools.cisco.com/ITDIT/MIBS/

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

This document is to be used in conjunction with the documents listed in the "Related Documentation" section.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2015-2016 Cisco Systems, Inc. All rights reserved.